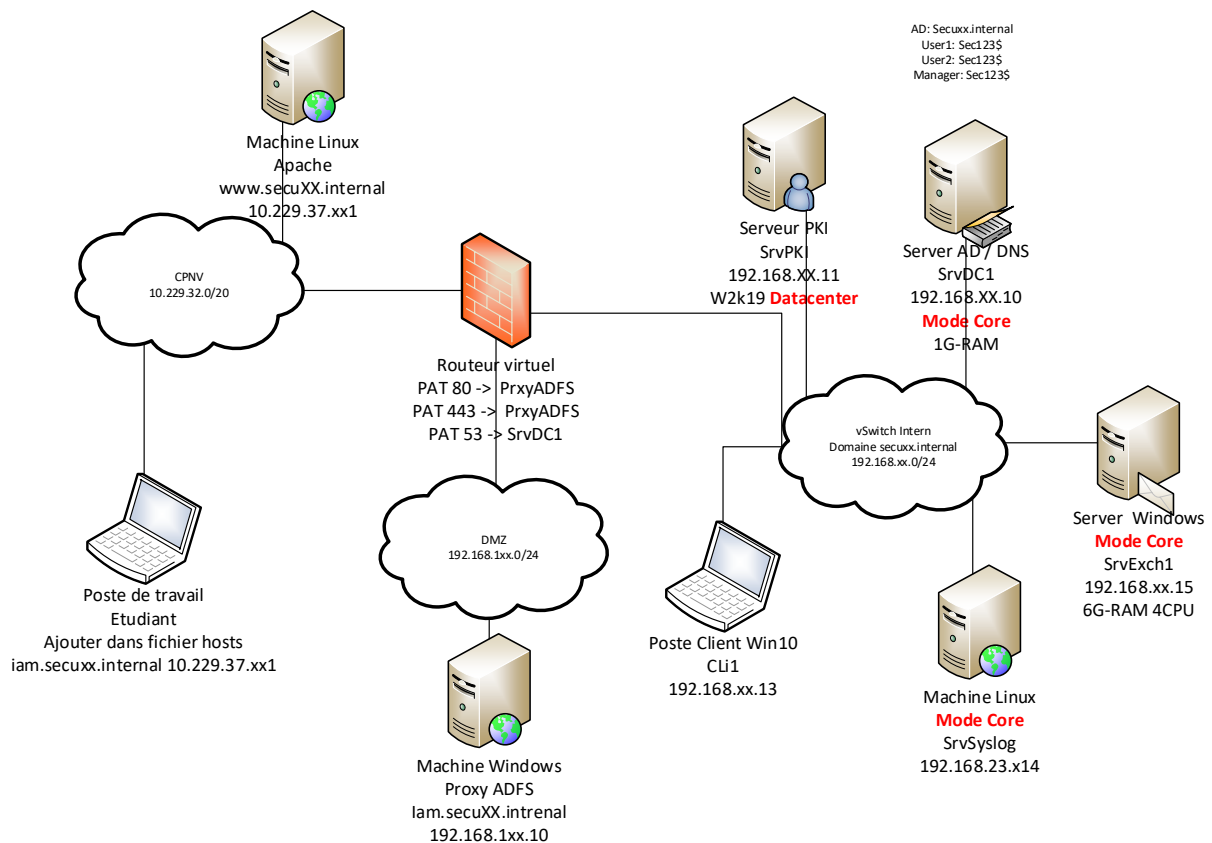


POC DMZ, rapport mise en service

Table des matières

POC DMZ, rapport mise en service	1
Schéma de l'infra :	1
User Story 1	2
User Story 2	2
User Story 3	2
User Story 4	3
User Story 5	4
User Story 6	4

Schéma de l'infra :



User Story 1

En tant qu'utilisateur du LAN j'aimerais accéder à Internet de manière sécurisée dans le but de ne pas compromettre la sécurité de mon entreprise.

Copie d'écran de la config du proxy dans le navigateur



User Story 2

En tant qu'utilisateur du LAN j'aimerais que mon navigateur soit configuré de manière automatique au niveau du proxy à utiliser, dans le but de se simplifier la vie.

Copie d'écran de la GPO



Copie d'écran du contenu du proxy.pac



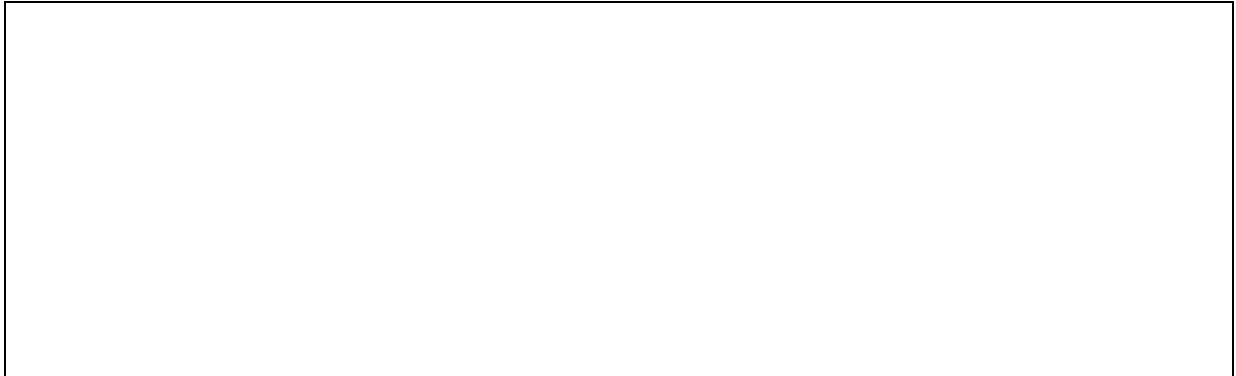
User Story 3

En tant que responsable de la sécurité, j'aimerais que les machines de mon infrastructure puissent communiquer en respectant les principes d'une DMZ, dans le but de sécuriser mon infrastructure contre la compromission d'une ou plusieurs machines.

Tableau des règles du firewall :

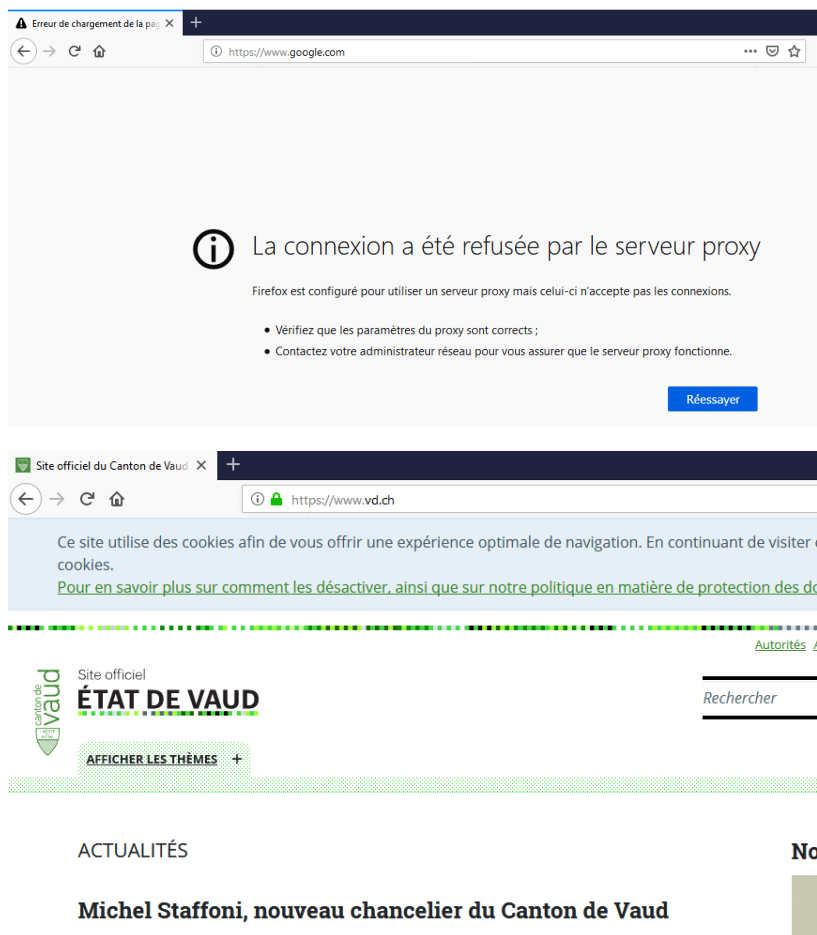
Source	Destination	Protocol	Action

Image avec les règles du firewall, (onglet Filter Rules de IP Firewall sur Winbox), mettez des commentaires dans les règles afin d'éclaircir la lecture



User Story 4

En tant que CTO, j'aimerais que les utilisateurs du LAN puissent surfer sur un nombre restreint de sites (www.cpnv.ch, www.vd.ch), pour améliorer leur productivité.



```

1701177199.032 0 192.168.23.100 TCP_DENIED/403 3832 CONNECT login.live.com:443 - HIER_NONE/- text/html
1701177199.048 0 192.168.23.100 TCP_DENIED/403 3832 CONNECT login.live.com:443 - HIER_NONE/- text/html
1701177243.448 0 192.168.23.100 TCP_DENIED/403 4132 CONNECT incoming.telemetry.mozilla.org:443 - HIER_NONE/- text/html
1701177243.795 0 192.168.23.100 TCP_DENIED/403 4102 CONNECT cdnjs.cloudflare.com:443 - HIER_NONE/- text/html
1701177243.824 0 192.168.23.100 TCP_DENIED/403 4102 CONNECT fonts.googleapis.com:443 - HIER_NONE/- text/html
1701177243.831 0 192.168.23.100 TCP_DENIED/403 4114 CONNECT www.googletagmanager.com:443 - HIER_NONE/- text/html
1701177244.360 0 192.168.23.100 TCP_DENIED/403 4114 CONNECT www.googletagmanager.com:443 - HIER_NONE/- text/html
1701177245.003 0 192.168.23.100 TCP_DENIED/403 4114 CONNECT www.google-analytics.com:443 - HIER_NONE/- text/html
1701177245.025 0 192.168.23.100 TCP_DENIED/403 4114 CONNECT www.google-analytics.com:443 - HIER_NONE/- text/html
1701177246.669 58 192.168.23.100 TCP_TUNNEL/200 1245 CONNECT prestations.vd.ch:443 - HIER_DIRECT/145.232.192.146 -
1701177247.263 0 192.168.23.100 TCP_DENIED/403 4114 CONNECT www.googletagmanager.com:443 - HIER_NONE/- text/html
1701177248.270 0 192.168.23.100 TCP_DENIED/403 4114 CONNECT www.google-analytics.com:443 - HIER_NONE/- text/html
1701177249.611 5919 192.168.23.100 TCP_TUNNEL/200 86777 CONNECT www.vd.ch:443 - HIER_DIRECT/145.232.192.197 -
1701177250.503 0 192.168.23.100 TCP_DENIED/403 4114 CONNECT www.google-analytics.com:443 - HIER_NONE/- text/html
1701177251.633 5676 192.168.23.100 TCP_TUNNEL/200 490 CONNECT statsweb.vd.ch:443 - HIER_DIRECT/145.232.192.131 -
1701177254.022 3681 192.168.23.100 TCP_TUNNEL/200 173214 CONNECT www.cpnv.ch:443 - HIER_DIRECT/128.65.195.179 -
1701177256.354 0 192.168.23.100 TCP_DENIED/403 3910 CONNECT tsfe.trafficshaping.dsp.mp.microsoft.com:443 - HIER_NONE/- text/html
1701177258.416 0 192.168.23.100 TCP_DENIED/403 3910 CONNECT tsfe.trafficshaping.dsp.mp.microsoft.com:443 - HIER_NONE/- text/html
1701177260.476 0 192.168.23.100 TCP_DENIED/403 3910 CONNECT tsfe.trafficshaping.dsp.mp.microsoft.com:443 - HIER_NONE/- text/html

```

User Story 5

En tant que responsable de la sécurité, j'aimerais que le LAN puisse accéder au WAN uniquement à l'aide de ping et protocoles web (https, http), dans le but de protéger l'infrastructure

```

Administrateur : Windows PowerShell
PS C:\Users\administrateur> ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . : secu23.internal
    Adresse IPv6 de liaison locale. . . . : fe80::4767:6df4:e6a0:425%4
    Adresse IPv4. . . . . : 192.168.23.100
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.23.1
PS C:\Users\administrateur> ping -n 1 8.8.8.8

Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=8 ms TTL=115

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 1, reçus = 1, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 8ms, Maximum = 8ms, Moyenne = 8ms
PS C:\Users\administrateur>

```

User Story 6

En tant que responsable informatique, je veux que les internautes puissent avoir accès à un site web dans le DMZ qui réponde à http://iam.secuxx.internal, dans le but de par la suite mettre en place un service d'authentification.

Image avec les règles du firewall, (onglet Nat Rules de IP Firewall sur Winbox), mettez des commentaires dans les règles afin d'éclaircir la lecture

